Act (FOIA)/Privacy Act (PA) Office, P.O. Box 648010, Lee's Summit, MO 64064–8010. Specific FOIA information can be found at *http://www.dhs.gov/foia* under ''Contacts.'' If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief FOIA Officer, Department of Homeland Security, 245 Murray Drive SW., Building 410, STOP–0655, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief FOIA Officer, *http://www.dhs.gov/foia* or 1–866–431–0486. In addition, you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

In processing requests for access to information in this system, USCIS will review the records in the operational system and coordinate with DHS to address access to records on the DHS unclassified and classified networks.

RECORD ACCESS PROCEDURES:

See ''Notification procedure'' above.

CONTESTING RECORD PROCEDURES:

See ''Notification procedure'' above.

RECORD SOURCE CATEGORIES:

DHS/USCIS obtains records from the benefit requestor, his or her Representative, Physician, Preparer, or Interpreter. DHS/USCIS personnel may input information as they process a case, including information from internal and external sources to verify whether a benefit requestor or family is eligible for the benefit requested. BIS also stores and uses information from the following USCIS, DHS, and other federal agency systems of records:

- DHS/USCIS/ICE/CBP–001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013);
- DHS/USCIS–002 Background Check Service, 72 FR 31082 (June 5, 2007);
- DHS/USCIS–003 Biometric Storage System, 72 FR 17172 (April 6, 2007);
- DHS/USCIS–005 Inter-Country Adoptions Security 72 FR 31086 (June 5, 2007);
- DHS/USCIS–006 Fraud Detection and National Security Records (FDNS) 77 FR 47411 (August 8, 2012);
- DHS/USCIS–010 Asylum Information and Pre-Screening, 75 FR 409 (January 5, 2010);
- DHS/CBP–011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008);
- DHS/ICE–001 Student and Exchange Visitor Information System, 75 FR 412 (January 5, 2010);
- DHS/ICE–011 Immigration and Enforcement Operational Records System (ENFORCE), 80 FR 24269 (April 30, 2015);
- DHS/CBP–021 Arrival and Departure Information System (ADIS), 80 FR 72081 (November 18, 2015);
- DHS/NPPD–004 DHS Automated Biometric Identification System (IDENT), 72 FR 31080 (June 5, 2007);
- JUSTICE/EOIR–001 Records and Management Information System, 72 FR 3410 (January 25, 2007);
- JUSTICE/FBI–002 The FBI Central Records System, 72 FR 3410 (January 25, 2007);
- JUSTICE/FBI–009 Fingerprint Identification Records System (FIRS), 72 FR 3410 (January 25, 2007);
- DOL/ETA–7 Employer Application and Attestation File for Permanent and Temporary Alien Workers, 77 FR 1728, (January 10, 2012);
- STATE–05 Overseas Citizens Services Records, 73 FR 24343 (May 2, 2008);
- STATE–26 Passport Records, 76 FR 34966 (July 6, 2011);
- STATE–39 Visa Records, 77 FR 65245 (October 25, 2012); and
- TREASURY/FMS–017 Collections Records, 74 FR 23006 (May 15, 2009).

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: October 5, 2016.

Jonathan R. Cantor,

Acting Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2016–25192 Filed 10–18–16; 8:45 am]

BILLING CODE 9111–97–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2016–0047]

Privacy Act of 1974; Department of Homeland Security/United States Citizenship and Immigration Services–017 Refugee Case Processing and Security Screening Information System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to establish a new Department of Homeland Security system of records titled, ''DHS/United States Citizenship and Immigration Services (USCIS)–017 Refugee Case Processing and Security Screening Information'' system of records. DHS/USCIS collects, uses, and maintains records on individuals seeking refugee status.

This newly established system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before November 18, 2016. This new system will be effective November 18, 2016.

ADDRESSES: You may submit comments, identified by docket number DHS–2016–0047 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 202–343–4010.
- *Mail:* Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to *http://www.regulations.gov*, including any personal information provided.

Docket: For access to the docket to read background documents or

comments received, please visit *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Donald K. Hawkins, (202) 272–8030, Privacy Officer, U.S. Citizenship and Immigration Services, 20 Massachusetts Avenue NW., Washington, DC 20529. For privacy questions, please contact: Jonathan R. Cantor, (202) 343–1717, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the DHS/USCIS proposes to establish a new DHS system of records titled, ''DHS/USCIS–017 Refugee Case Processing and Security Screening Information'' system of records.

A refugee is generally defined under U.S. law as a person who is outside his or her country of origin and is unable or unwilling to return because of past persecution or a well-founded fear of future persecution on account of race, religion, nationality, political opinion, or membership in a particular social group. In certain instances, under U.S. law, persons within their countries of nationality or habitual residence may be considered refugees for the purpose of admission to United States. The U.S. Refugee Admissions Program (USRAP) was created by the Executive Branch and authorized by Congress to admit foreign nationals who are outside the United States as refugees. An applicant must first be given access to the USRAP before he or she can be considered for eligibility as a refugee. The USRAP is an interagency partnership involving federal agencies, such as the Department of State (DOS) and DHS, and international and nongovernmental organizations working together, both overseas and domestically, to identify and admit qualified refugees for resettlement into the United States. Within DHS, USCIS has responsibility for adjudicating applications for refugee status and reviewing case decisions, and U.S. Customs and Border Protection (CBP) screens arriving refugees for admission at the port of entry.

Data on refugee applications are entered into the DOS-owned and operated Worldwide Refugee Admissions Processing System (WRAPS), which is an electronic case management system for refugee resettlement that is used by DOS Bureau of Population, Refugees, and Migration (PRM) and its worldwide partners and facilitates the refugee resettlement process. WRAPS contains case information and tracks the processing of refugee applications as they move through the required administrative and adjudicative steps until arrival in the United States.

USCIS is responsible for determining applicants' eligibility for refugee status based on in-person interviews with USCIS adjudicators. Refugee applicants are also subject to numerous biographic and biometric security checks. Refugees are considered for resettlement in the United States if they meet one of the three processing priorities established by DOS:

(1) The Office of the United Nations High Commissioner for Refugees (UNHCR), a U.S. Embassy, or a specially trained non-governmental organization refers them to the United States for resettlement consideration;

(2) Groups of special concern identified by the USRAP; or

(3) Family reunification cases (*i.e.*, spouses, unmarried children under 21, parents of persons lawfully admitted to the United States as refugees or asylees, or persons who are lawful permanent residents or U.S. citizens who previously had refugee or asylum status for designated nationalities).

Generally, refugees must be outside their country of origin or last habitual residence to be eligible for access to the USRAP; however the USRAP has legal authority to process refugees in their home countries in certain locations.

All refugee applicants, derivatives, and certain family members are subject to background security checks. As part of this process, refugee applicants undergo a series of biometric and biographic checks. USCIS may provide enhanced review and screening of certain refugee cases. Through close coordination with the federal law enforcement and intelligence communities, these checks are continually reviewed and enhanced. Additionally, in some instances these checks may involve reviewing social media to identify information on applicants related to national security concerns and/or the refugee eligibility determination.

If the USCIS adjudicator finds that the individual qualifies as a refugee and meets other U.S. admission criteria, the officer will approve or conditionally approve the refugee's application for resettlement and submit it to the Resettlement Support Center (RSC) for further processing. Conditional approvals become final once the results of all background checks have been received and reviewed by USCIS. Upon arrival in the United States, and after admission by a CBP Officer, USCIS creates the A-Files from the refugee travel packet and from documents forwarded from the RSC.

Individuals admitted to the United States as a refugee are required to apply for adjustment of status to that of a lawful permanent resident one year after admission as refugees. Until adjustment of status, persons admitted as refugees possess ''refugee status,'' unless such status is terminated by USCIS. Employment authorization for refugees admitted to the United States is incidental to refugee status. A refugee admitted to the United Statement may request derivative refugee status for his/her spouse and unmarried children under the age of 21 within two years of admission as a refugee by filing Form I–730, *Refugee/Asylee Relative Petition.* Refugees who wish to travel abroad may obtain a refugee travel document in order to facilitate their return to the United States. USCIS is also responsible for processing applications for permanent residency, employment authorization, and refugee travel documents, which are processed in the Computer Linked Applications Management System 3 (CLAIMS 3) and Case and Activity Management for International Operations (CAMINO). More information on these systems is available at *www.dhs.gov/privacy.* Benefit request forms are stored in either the A-File or Receipt File.

USCIS has established the Refugee Case Processing and Security Screening Information system of records to facilitate intake, adjudication, and review of refugee programs. USCIS uses Refugee Case Processing and Security Screening Information to track case status, as well as initiate, facilitate, and track biometric and biographic check screenings and to prevent the approval of any benefit prior to the review and completion of all background checks. Finally, these records are used by USCIS to generate statistical reports to assist with oversight of production and processing goals.

As a matter of policy, the regulations at 8 CFR 208.6 prohibiting disclosure of information contained in or pertaining to an alien's application for asylum, credible fear determination, or reasonable fear determination are applied to an alien's application or status as a refugee. USCIS affords information covered by the DHS/USCIS–017 Refugee Case Processing and Security Screening Information System SORN the confidentiality protections contained in 8 CFR 208.6, which strictly limits the disclosure of information to third parties. Information protected by 8 CFR 208.6 may not be disclosed without the written consent of the applicant,

except as permitted by 8 CFR 208.6(c) or at the discretion of the Secretary of Homeland Security or the Attorney General of the United States.

Consistent with DHS's information sharing mission, information covered by the DHS/USCIS–017 Refugee Case Processing and Security Screening Information SORN may be shared with other DHS components that have a need-to-know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/USCIS may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the confidentiality provisions of 8 CFR. 208.6 and with the routine uses set forth in this system of records notice.

This new system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a ''system of records.'' A ''system of records'' is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is the description of the DHS/USCIS–017 Refugee Case Processing and Security Screening Information System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

System of Records

Department of Homeland Security (DHS)/United States Citizenship and Immigration Services (USCIS)–017

SYSTEM NAME:

DHS/USCIS–017 Refugee Case Processing and Security Screening Information

SECURITY CLASSIFICATION:

Unclassified, Sensitive, For Official Use Only. The data may be retained on classified networks, but this does not change the nature and character of the data until it is combined with classified information.

SYSTEM LOCATION:

Records are maintained in DHS/USCIS information technology (IT) systems and associated electronic and paper files located at USCIS Headquarters in Washington, DC and in DHS/USCIS service centers and domestic and international field offices to support USCIS Refugee, Asylum, and International Operations (RAIO) Refugee Affairs Division (RAD). The DHS/USCIS IT systems, as well as DOS IT systems that support the Refugee Case Processing and Security Screening Information include: The DOS WRAPS, USCIS CAMINO, and CLAIMS 3. Refugee application data and biographic check results for the principal applicant, derivatives, and other family members are processed in DOS WRAPS and USCIS CAMINO. Biometric check results for the refugee applicant and derivatives are stored in the USCIS Customer Profile Management System (CPMS). Applications for the adjustment of status, refugee travel documents, and follow-to-join benefit petitions Form I–730, are processed in USCIS CAMINO and CLAIMS 3. Records are replicated from the operational DHS/USCIS IT systems and maintained on DHS unclassified and classified networks.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include: (1) Individuals who have applied for admission to the United States under the USRAPS; (2) spouses (current and former) and children of a principal refugee applicant included in the refugee application; (3) principal refugee applicant's parents and relatives in the United States; (4) other individuals listed as part of the family tree and including points of contact in the United States and other individuals with whom the applicant associates; (5) individuals who have petitioned for follow-to-join (derivative) refugee or asylum status for their spouse and unmarried children under the age of 21 on Form I–730 *Refugee/Asylee Relative Petition;* (6) persons who complete refugee applications on behalf of the refugee applicant (*e.g.*, form preparers, interpreters); and (7) individuals associated with partner organizations such as Resettlement Support Centers and the United Nations High Commissioner for Refugees.

CATEGORIES OF RECORDS IN THE SYSTEM:

Information about benefit requestor and derivatives may include:

- Full name;
- Alias(es);
- Physical and mailing addresses;
- Date of birth;
- Place of birth;
- Gender;
- Ethnicity or tribal group;
- Religion;
- Present Citizenship or Nationality;
- Alien Number (A–Number);
- Resettlement Support Center Case Number;
- Receipt Number;
- USCIS Online Account Number;
- Social Security number (SSN), if any;
- Relationship to benefit requestor (*i.e.*, children under the age of 21 and spouse);
- Employment authorization eligibility and application history;
- Records regarding organization membership or affiliation;
- Supporting documentation as necessary (*e.g.*, birth, marriage, divorce certificates; licenses; academic diplomas; academic transcripts; appeals or motions to reopen or reconsider decisions; explanatory statements; and unsolicited information submitted voluntarily by the applicant or family members in support of a benefit request);
- Government-issued identification (*e.g.*, passport, driver license):
  - Document type;
  - Issuing organization;
  - Document number;
  - Expiration date;
  - Benefit requested;
- Notices and communications, including:
  - Receipt notices;
  - Requests for Evidence;
  - Notices of Intent to Deny;
  - Proofs of benefit;
- Phone and fax numbers;
- Email addresses;
- Social Media handles, associated identifiable information, and results;
- Marital status;
- Place of marriage;
- Arrival/Departure information;
- Immigration history (*e.g.*, citizenship/naturalization certificate number, removals, explanations);
- Family relationships (*e.g.*, parent, spouse, sibling, child, other dependents);
- Relationship practices *(e.g.*, polygamy, custody, guardianship);
- Personal background information (*e.g.*, involvement with national security threats, criminal offenses, Communist party affiliation, activity and/or affiliation with groups or organizations

abroad, torture, genocide, killing, injuring, forced sexual contact, limiting or denying others religious beliefs, service in military or other armed groups, work in penal or detention systems, weapons);

- Health information (*e.g.*, vaccinations, referrals, communicable diseases, physical or mental disorders, prostitution, drug or alcohol abuse);
- Employment authorization eligibility and application history;
- Professional accreditation information;
- Financial information (*e.g.*, income, expenses, scholarships, savings, assets, property, financial support, supporter information, life insurance, debts, encumbrances, tax records);
- Travel history;
- Explanation/description of foreign travel;
- Education history;
- Work history;
- Documents establishing identity and claimed relationship (*e.g.*, marriage record, civil or criminal history, medical records, education records, DNA results);
- Physical description (*e.g.*, height, weight, eye color, hair color, race, ethnicity, identifying marks like tattoos or birthmarks);
- Biometrics (*i.e.*, fingerprints and photographs) and other information (*e.g.*, race, ethnicity, weight, height, eye color, hair color);
- Background check results;
- Reports of investigations or derogatory information obtained from DHS and other federal systems;
- Refugee interview notes and assessments;
- Information regarding the status of Department of Justice (DOJ), Executive Office of Immigration Review (EOIR) proceedings, if applicable; and
- Case processing information such as date applications were filed or received by USCIS; application/petition status, location of record, other control number when applicable, and fee receipt data.

Information about the benefit requestor's parents and relatives in the United States and other individuals listed as part of the family tree and including points of contact in the United States and other individuals with whom the applicant associates:

- Name;
- Date of Birth;
- Relationship to the benefit requestor;
- Country of Birth;
- Address; and
- Background check results.

Information about Registrants, Preparers, and Interpreters may include:

- Full name;
- Organization;
- Business State ID number;
- Employer Tax Identification Number;
- Physical and mailing addresses:
- Email address;
- Phone and fax numbers;
- Relationship to applicant; and
- Signature.

Information about Accredited Representatives and Attorneys includes:

- Name;
- Law Firm/Recognized Organization;
- Physical and mailing addresses:
- Phone and fax numbers;
- Email address;
- Attorney Bar Card Number or equivalent;
- Bar membership;
- Accreditation date;
- Board of Immigration Appeals Representative Accreditation;
- Expiration date;
- Law Practice Restriction Explanation; and
- Signature.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintaining this system is in Section 207 of the Immigration and Nationality Act (INA), as amended.

PURPOSE(S):

The purpose of this system is to collect, use, maintain, disseminate, and store refugee information, including the administration and adjudication of the review of refugee applications and follow-to-join applications for those who are seeking consideration for refugee resettlement, as well as applications for permanent residency, employment authorization, and travel abroad.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3). Even when a valid routine use permits disclosure of information from this system of records to a third party, in some cases such disclosure may not be permissible because of confidentiality laws and policies that limit the sharing of information regarding individuals applying for refugee status.

Information in this system of records contains information relating to persons who have pending or approved refugee applications or pending or approved follow-to-join petitions should not be disclosed pursuant to a routine use unless disclosure is otherwise permissible under 8 CFR 208.6. These confidentiality provisions do not prevent DHS from disclosing information to the DOJ and Offices of the United States Attorneys as part of an ongoing criminal or civil investigation. These provisions permit disclosure to courts under certain circumstances as well, as provided under 8 CFR 208.6(c)(2). Subject to these restrictions:

A. To the DOJ, including Offices of the United States Attorneys, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party of the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or other Federal Government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed

compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To DOS, their contractors, agents, grantees, experts, consultants, or others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DOS (*e.g.*, RSC, International Organization for Migration), when necessary to accomplish refugee case processing.

I. To federal and foreign government intelligence or counterterrorism agencies or components when DHS becomes aware of an indication of a threat or potential threat to national or international security, or when such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

J. To requesting foreign governments under appropriate information sharing agreements and there is a legitimate need to share information for law enforcement or national security purposes under 8 CFR 208.6.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

DHS/USCIS stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

RETRIEVABILITY:

DHS/USCIS may retrieve records by any of the data elements listed above or a combination thereof. This may include name, date of birth, alias(es), place of birth, gender, ethnicity or tribal group, physical addresses, relatives addresses, A-Number, SSN, USCIS Online Account, Receipt Number, Resettlement Support Center Case Number, government-issued identification, notices and communications, phone numbers, and email addresses.

SAFEGUARDS:

DHS/USCIS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS/USCIS has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RETENTION AND DISPOSAL:

DHS/USCIS stores the physical documentation in the Alien File, and maintains refugee case processing and security screening information and follow-to-join applications in the respective case management systems. The A-File records are permanent whether hard copy or electronic. USCIS transfers the A-Files to the custody of NARA 100 years after the individual's date of birth.

NARA approved the CAMINO [N1–566–12–06] and CLAIMS 3 [N1–566–08–12] Retention Schedules.

CAMINO Master File automated records are maintained for 25 years after the case is closed and then destroyed.

CLAIMS 3 records are destroyed after the data is transferred to the electronic master file and verified. Information in the master file is destroyed 15 years after the last completed action with respect to the benefit. USCIS is proposing to update the CLAIMS 3 Retention Schedule to destroy records 50 years after the last completed action. This retention schedule allows USCIS to address any follow-up inquiries or requests related to the application, including inquiries related to law enforcement, public safety, and national security, and to respond to Freedom of Information Act/Privacy Act (FOIA/PA) matters.

The biometric check data is retained in CPMS, which is governed by a DHS-wide retention schedule. The records in CPMS are retained for 100 years from the individual's data of birth in accordance with the NARA Disposition Authority Number DAA–0563–2013–0001–0005.

SYSTEM MANAGER AND ADDRESS:

For refugee records, the DHS system manager is the Chief, Refugee Affairs Division, Refugee, Asylum, and International Operations Directorate, U.S. Citizenship and Immigration Services, Department of Homeland Security, 111 Massachusetts Avenue NW., Washington, DC 20529.

For refugee follow-to-join records, the DHS system manager is the Chief, International Operations Division, Refugee, Asylum, and International Operations Directorate, U.S. Citizenship and Immigration Services, Department of Homeland Security, 111 Massachusetts Avenue NW., Washington, DC 20529.

For refugee records relating to adjustment of status and travel, the DHS system manger is the Associate Director, Service Center Operations Directorate, U.S. Citizenship and Immigration Services, Department of Homeland Security, 111 Massachusetts Avenue NW., Washington, DC 20529.

NOTIFICATION PROCEDURE:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the National Records Center (NRC) FOIA/PA Office, P.O. Box 648010, Lee's Summit, MO, 64064–8010, whose contact information can be found at *http://www.dhs.gov/foia* under ''Contacts.'' If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive SW., Building 410, STOP–0655, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief

Freedom of Information Act Officer, *http://www.dhs.gov/foia* or 1–866–431–0486. In addition, you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURES:

See ''Notification procedure'' above.

CONTESTING RECORD PROCEDURES:

See ''Notification procedure'' above.

RECORD SOURCE CATEGORIES:

DHS/USCIS obtains records from the applicant, and his or her accredited representative, preparer, or interpreter. Other information sources include family members, federal databases for security screening checks, RSCs, the DOS Refugee Processing Center, resettlement agencies, international organizations, and local sources at overseas sites. DHS/USCIS personnel may input information as they process a case, including information from internal and external sources to verify whether a benefit requestor or family is eligible for the refugee benefit requested. Refugee Case Process and Security Screening also stores and uses information from the following USCIS, DHS, and other federal agency systems of records:

- DHS/USCIS/ICE/CBP–001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013);
- DHS/USCIS–002 Background Check Service, 72 FR 31082 (June 5, 2007);
- DHS/USCIS–003 Biometric Storage System, 72 FR 17172 (April 6, 2007);
- STATE–05, Overseas Citizen Services Records (May 2, 2008);
- STATE–26, Passport Records, (Mar. 24, 2015)STATE–39, DOS Visa Opinion Information Service (VOIS), 77 FR 65245, (Oct. 25, 2012);
- JUSTICE/FBI–002 The FBI Central Records System, 72 FR 3410 (January 25, 2007);
- DoD/A0025–2 Defense Biometric Services, 74 FR 48237, (September 22, 2009);
- DoD Detainee Biometric Information System, 72 FR 14534, (March 28, 2007); and
- DoD/A0025–2a Defense Biometric Identification Records System, 74 FR 17840, (April 17, 2009).

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: October 5, 2016.

Jonathan R. Cantor,

Acting Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2016–25195 Filed 10–18–16; 8:45 am]

BILLING CODE 9111–97–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2016–0073]

Privacy Act of 1974; Department of Homeland Security United States Immigration Customs and Enforcement—011 Criminal Arrest Records and Immigration Enforcement Records System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to update, rename, and reissue a current DHS system of records titled, ''DHS// U.S. Immigration and Customs Enforcement (ICE)–011 Immigration and Enforcement Operational Records (ENFORCE)'' system of records. DHS/ICE collects, uses, and maintains ENFORCE to support the identification, apprehension, and removal of individuals unlawfully entering or present in the United States in violation of the Immigration and Nationality Act, including fugitive aliens. DHS/ICE also uses ENFORCE to support the identification and arrest of individuals (both citizens and non-citizens) who commit violations of federal criminal laws enforced by DHS. This system of records is being created from a previously issued system of records, DHS/ICE 011–Immigration and Enforcement Operational Records (ENFORCE). *See* 80 FR 24,269 (Apr. 30, 2015).

DHS/ICE is updating this system of records to: Change the system of records name to ''DHS/ICE–011 Criminal Arrest Records and Immigration Enforcement Records (CARIER)'' System of Records; update and reorganize the categories of individuals for clarity; expand the categories of records to include recordings of detainee telephone calls and information about these calls, as well as information related to detainees' accounts for telephone or commissary services in a detention facility; update the system manager; clarify system location; and add twenty-five routine uses and modify twenty routine uses to describe how the Department of Homeland Security may share information from this system. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

This updated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before November 18, 2016. This updated system will be effective November 18, 2016.

ADDRESSES: You may submit comments, identified by docket number DHS–2016–0073 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 202–343–4010.
- *Mail:* Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received, please visit *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Amber Smith, (202–732–3300), Privacy Officer, U.S. Immigration and Customs Enforcement, 500 12th Street SW., Mail Stop 5004, Washington, DC 20536. For privacy questions, please contact: Jonathan R. Cantor, (202–343–1717), Acting Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION: